初等数论

整数的基本性质

设a,b是两个整数，其中b != 0。如果存在一个整数q使得等式 a = bq成立，就称b整除a或者a被b整除记作b|a，并把b叫作a的因数，把a叫作b的倍数。这时，q也是a的因数，我们常常将q写成a / b;
在C++中用 a % b == 0表示整除

整除的一些常用结论:

1. 当b遍历整数a的所有因数时，-b也遍历也遍历整数a的所有因数
2. 当b遍历整数a的所有因数时，a/b也遍历整数a的所有因数
   所以对于此来说 1~sqrt(a)的因子和sqrt(a) + 1 ~ a的因子一一对应
   所以我们求数a的因子有哪些的代码通常这样写

   ```
   for(int i = 2; i * i <= a; i++){
       if(a % i != 0) continue;
       if(i * i == a) b[++cnt] = i;
       else b[++cnt] = i,b[++cnt] = a / i;
   }
   ```

3. 设b，c都是非零整数
   1. 若b | a，则 |b| | |a|
   2. 若 b | a，则 bc | ac
   3. 若 b | a，则 1< |b| <= |a|
   4. 若 b | a，a | c 那么 b | c
   5. 若 b | a，b | c 那么任意 整数x，y使得 b | ax + cy
   6. 设 a != 0,b = qa + c 那么 a | b $\Longleftrightarrow$ a| c

---

练习:

1.苹果丰收，得到了120个苹果，恰好平分给x个小朋友（每个小朋友拿到的苹果数量一样) 请问，x能取那些值

2.找循环节。给定一个长度为n的字符串，求它的最小循环节长度，n <= 10^5。例如输入 "abbaabbaabba" 输出4

3.洛谷P2926。给定n和n个正整，求每个数是另外多少个数的倍数，n <= 10^5，其他数字a_i不超过10^6。例如给出5个数，分别是2，1，2，3，4。答案输出 2，0，2，1，3

4.洛谷P1403

> 小联最近在研究和约数有关的问题，他统计每个正数 N 的约数的个数，并以 $f(N)$ 来表示。例如 12 的约数有 $1,2,3,4,6,12$，因此 $f(12)=6$。下表给出了一些 $f(N)$ 的取值：
>
> | N | 1 | 2 | 3 | 4 | 5 | 6 |
> | --- | --- | --- | --- | --- | --- | --- |
> | $f(N)$ | 1 | 2 | 2 | 3 | 2 | 4 |
>
> 现在请你求出：
>
> $$\sum_{i=1}^{n} f(i)$$

N <= 10^6

拓展:

> 小联最近在研究和约数有关的问题，他统计每个正数 N 的约数的个数，并以 $f(N)$ 来表示。例如 12 的约数有 $1,2,3,4,6,12$，因此 $f(12)=6$。下表给出了一些 $f(N)$ 的取值：
>
> | N | 1 | 2 | 3 | 4 | 5 | 6 |
> | --- | --- | --- | --- | --- | --- | --- |
> | $f(N)$ | 1 | 2 | 2 | 3 | 2 | 4 |
>
> 现在请你求出：
>
> $$\sum_{i=1}^{n} f(i)$$

N <= 10^9

洛谷P2424

> Smart 最近沉迷于对约数的研究中。
>
> ## 题目描述
>
> 对于一个数 X，函数 $f(X)$ 表示 X 所有约数的和。例如：$f(6)=1+2+3+6=12$。对于一个 X，Smart 可以很快的算出 $f(X)$。现在的问题是，给定两个正整数 $X,Y(X<Y)$，Smart 希望尽快地算出 $f(X)+f(X+1)+......+f(Y)$的值，你能帮助 Smart 算出这个值吗？
>
> ## 输入格式
>
> 输入文件仅一行，两个正整数 X 和 $Y(X<Y)$，表示需要计算 $f(X)+f(X+1)+\cdots+f(Y)$。
>
> ## 输出格式
>
> 输出只有一行，为 $f(X)+f(X+1)+\cdots+f(Y)$ 的值。

X,Y <= 10^9

素数

设n为一个正整数且n != 1，倘若n的因子只有自己本身和1的话他就是个素数(又称质数，不可约数)，其他的数称为合数

特殊的 0，1既不是质数也不是合数，所以最小的质数是2，最小的合数是4

规定:若没有特殊说明，素数一般指正整数，用p_1,p_2.....p_n表示

p 和 -p总是同为素数或者同为合数。**如果没有特别说明，素数总是指正的素数。**

整数的因数是素数，则该素数称为该整数的素因数（素约数）。

素数与合数的简单性质：

- 大于1的整数a是合数，等价于a可以表示为整数d 和e（1<d,e<a）的乘积。
- 如果素数p有大于1的约数 d，那么 d = p 。
- 大于1的整数a一定可以表示为素数的乘积。
- 对于合数a，一定存在素数 p <= $\sqrt{a}$使得 p | a。
- 素数有无穷多个。

- 所有大于3的素数都可以表示为6n±1 的形式。
  证明:当n表示自然数的时候，用6n、6n+1、6n+2、6n+3、6n+4、6n+5就可以表示所有的自然数。其中，6n是6的倍数，一定不是质数；
  6n+2是偶数，只有n=0时，6n+2=2是质数；
  6n+3是3的倍数，只有n=0时，6n+3=3是质数；
  6n+4是偶数，并且大于2，一定不是质数；
  所以，在n > 0的情况下，只有6n+1和6n+5才可能是质数。
  而6n+5也可以用6n–1表示，如n=1时，6n+5=11； n =2时，6n–1=11。
  这就证明了，大于3质数，都是形如6n+1或6n–1的数。

若gcd(a,b,c,d) = 1 则称 a,b,c,d互素(质数)

算术基本定理:任何一个大于1的自然数N,如果N不为质数，那么N可以唯一分解成有限个质数的乘积.

x = $p_1^{a_1}$ * $p_2^{a_2}$ * ….. * $p_n^{a_n}$

存在性证明:

反证法

假设存在不能**分解成有限个质数**的乘积的合数，则其中必有一个**最小**的数（最小数原理）设为n.

n不是**质数**，所以存在大于1小于n的自然数a,b，使n=ab.

∃a,b∈N∧1<a,b<n⇒n=ab

- 如果a，b都为**质数**，与假设矛盾.
- 如果a，b**至少**有一个是**合数**,因为都比n要小，所以这个合数一定可以被分解成有限个质数的乘积，将乘积替换，可推出n可以分解成有限个质数的乘积，与假设矛盾.

所以原命题成立.

唯一性证明:

反证法

欧几里得引理：如果 p是素数且p|bc，那么p|b或者p|c.

假设存在某些数，它们有能分解为两种**不同**的质数乘积，将其中**最小**的数设为n

$n = p_1p_2p_3\cdots p_r = q_1q_2q_3\cdots q_s$

因为p_1可以除以$(q_1)(q_2q_3\cdots q_s)$,由欧几里得引理得出$p_1 \mid q_1$或者$p_1 \mid q_2q_3\cdots q_s$ （注意这里设的p和q全为**质数**）

所以可以得到 $p_1 = q_1$或者$p_1 = q_i$(2≤i≤s,i∈k)

上面任意一种情况，等可以将原式子左右两边同时**消掉**一个数，这样就得到了**一个更小的数**能表示两种质数乘积，与**n是最小数**的假设矛盾，唯一性得证.

练习:

1. 给定 n 个正整数 a_i，判定每个数是否是质数。 n <= 100, a_i <= 1e9

2. 给定 n 个正整数 a_i，将每个数分解质因数，并按照质因数从小到大的顺序输出每个质因数的底数和指数。 n <= 100, a_i <= 1e9

3. 洛谷U248208给定一个正整数 n，请你求出 1~n 中质数的个数。 n <= 1e6

4. 给定一个正整数 n，请你求出 1~n 中质数的个数。 n <= 1e7

5. **U248212哥德巴赫猜想的内容如下:**

   任意一个大于 4 的偶数都可以拆成两个奇素数之和。

   例如:

   8=3+5

   20=3+17=7+13

   42=5+37=11+31=13+29=19+23

   现在，你的任务是验证所有小于一百万的偶数能否满足哥德巴赫猜想。 n<=1e6

余数

余数的定义：设 a,b 为两个给定的整数，$a \neq 0$。设 d 是一个给定的整数。那么，一定存在唯一的一对整数 q 和 r，满足 $b = qa + r, d \leq r < |a| + d$。

无论整数 d 取何值，r 统称为余数。$a \mid b$ 等价于 $a \mid r$。

一般情况下，d 取 0，此时等式 $b = qa + r, 0 \leq r < |a|$ 称为带余数除法（带余除法）。这里的余数 r 称为最小非负余数。

余数往往还有两种常见取法:

绝对最小余数：d 取 a 的绝对值的一半的相反数。即 $b = qa + r, -\frac{|a|}{2} \leq r < |a| - \frac{|a|}{2}$。

最小正余数：d 取 1。即 $b = qa + r, 1 \leq r < |a| + 1$。

带余数除法的余数只有最小非负余数。**如果没有特别说明，余数总是指最小非负余数。**

余数的性质:

- 任一整数被正整数 a 除后，余数一定是且仅是 0 到 $(a-1)$ 这 a 个数中的一个。
- 相邻的 a 个整数被正整数 a 除后，恰好取到上述 a 个余数。特别地，一定有且仅有一个数被 a 整除。

运算取mod：设$a_1 = b * k_1 + c_1 \quad a_2 = b * k_2 + c_2$
$(a_1 + a_2)$b=$(c1 + c2)$ % b
$(a_1$ % b +a_2 % b) % b = $(c1 + c2)$ % b
所以$(a_1 + a_2)$ % b = $(a_1$% b + a_2 % b) % b
$(a_1$ % $b * a_2$ % b) % b = $(c_1 * c_2)$ % b

$a_1 * a_2$ % b = $(b^2 * k_1 * k_2 + c_1 * b * k_2 + c_1 * c_2)$ % b = $(c_1 * c_2)$ % b
所以(a_1 % $b * a_2$% b) % b = $(c_1 * c_2)$ % b

练习:

1. 洛谷U248267 给定两个整数a,b输出a^1，a^2....，a^b，输出可能很大所以答案对于1e9+7取模 a,b <= 10^6

同余

同余的定义：设整数m≠0。若m | (a - b)，称m为模数（模），a同余于b模m，b是a对模m的剩余。记作 a ≡b(mod m)。
否则，a不同于b模m，b不是a对模m的剩余。
这样的等式，称为模m的同余式，简称同余式。
根据整除的性质， a ≡b(mod -m) **如果没有特别说明模数一般是正整数**
式中的b是a对模m的剩余，这个概念与余数完全一致。通过限定b的范围，相应的有a对模m的最小非负剩余、绝对最小剩余、最小正剩余。

同余的性质:

- 自反性：$a \equiv a \pmod m$。
- 对称性：若 $a \equiv b \pmod m$，则 $b \equiv a \pmod m$。
- 传递性：若 $a \equiv b \pmod m, b \equiv c \pmod m$，则 $a \equiv c \pmod m$。
- 线性运算：若 $a, b, c, d \in \mathbf{Z}, m \in \mathbf{N}^*, a \equiv b \pmod m, c \equiv d \pmod m$ 则有：
  - $a \pm c \equiv b \pm d \pmod m$。
  - $a \times c \equiv b \times d \pmod m$。
- 若 $a, b \in \mathbf{Z}, k, m \in \mathbf{N}^*, a \equiv b \pmod m$, 则 $ak \equiv bk \pmod{mk}$。
- 若 $a, b \in \mathbf{Z}, d, m \in \mathbf{N}^*, d \mid a, d \mid b, d \mid m$，则当 $a \equiv b \pmod m$ 成立时，有 $\frac{a}{d} \equiv \frac{b}{d} \left(\bmod \frac{m}{d}\right)$。
- 若 $a, b \in \mathbf{Z}, d, m \in \mathbf{N}^*, d \mid m$，则当 $a \equiv b \pmod m$ 成立时，有 $a \equiv b \pmod d$。
- 若 $a, b \in \mathbf{Z}, d, m \in \mathbf{N}^*$，则当 $a \equiv b \pmod m$ 成立时，有 $\gcd(a, m) = \gcd(b, m)$。若 d 能整除 m 及 a, b 中的一个，则 d 必定能整除 a, b 中的另一个。

乘法逆元: 如果一个线性同余方程ax ≡1(mod b) ，则称x为a mod b的逆元，记作a^{-1}

证明

对于 $\forall p \in \mathbf{Z}$，有 $1 \times 1 \equiv 1 \pmod p$ 恒成立，故在 p 下 1 的逆元是 1，而这是推算出其他情况的基础。

其次对于递归情况 i^{-1}，我们令 $k = \lfloor \frac{p}{i} \rfloor$，$j = p \bmod i$，有 $p = ki + j$。再放到 $\mod p$ 意义下就会得到：$ki + j \equiv 0 \pmod p$；

两边同时乘 $i^{-1} \times j^{-1}$：

$kj^{-1} + i^{-1} \equiv 0 \pmod p$

$i^{-1} \equiv -kj^{-1} \pmod p$

再带入 $j = p \bmod i$，有 $p = ki + j$，有：

$i^{-1} \equiv -\lfloor \frac{p}{i} \rfloor (p \bmod i)^{-1} \pmod p$

我们注意到 $p \bmod i < i$，而在迭代中我们完全可以假设我们已经知道了所有的模 p 下的逆元 $j^{-1}, j < i$。

故我们就可以推出逆元，利用递归的形式，而使用迭代实现：

$$i^{-1} \equiv \begin{cases} 1, & \text{if } i = 1, \\ -\lfloor \frac{p}{i} \rfloor (p \bmod i)^{-1}, & \text{otherwises.} \end{cases} \pmod p$$

```
inv[1] = 1;
for (int i = 2; i <= n; ++i) {
  inv[i] = (long long)(p - p / i) * inv[p % i] % p;
}
```

练习：

1. 洛谷P3811给定一个数n求解 1 ~ n每个数的逆元，n <= 3e6

约数

其实上边讲整除的时候讲过一部分了，但是这里主要是做练习

练习：

1. 洛谷U248278 给定 n 个正整数 a_i，请你输出这些数的乘积的约数个数，答案对 10^9+7取模。

2. 洛谷U248283 给定 n 个正整数 a_i，请你输出这些数的乘积的约数之和，答案对 10^9+7取模。

最大公约数

如果我们已知两个数a和b，如何求出二者的最大公约数呢?

不妨设 a > b

我们发现如果b是a的约数，那么b就是二者的最大公约数。 下面讨论不能整除的情况，即a = b * q + r ，其中 r < b。

我们通过证明可以得到 gcd(a,b) = gcd(b,a mod b)，过程如下

> 设 $a=bk+c$，显然有 $c=a \bmod b$。设 $d \mid a$，$d \mid b$，则 $c=a-bk, \frac{c}{d}=\frac{a}{d}-\frac{b}{d}k$。
>
> 由右边的式子可知 $\frac{c}{d}$ 为整数，即 $d \mid c$ 所以对于 a,b 的公约数，它也会是 $a \bmod b$ 的公约数。
>
> 反过来也需要证明:
>
> 设 $d \mid b$，$d \mid (a \bmod b)$，我们还是可以像之前一样得到以下式子 $\frac{a \bmod b}{d}=\frac{a}{d}-\frac{b}{d}k, \frac{a \bmod b}{d}+\frac{b}{d}k=\frac{a}{d}$。
>
> 因为左边式子显然为整数，所以 $\frac{a}{d}$ 也为整数，即 $d \mid a$，所以 $b, a \bmod b$ 的公约数也是 a,b 的公约数。
>
> 既然两式公约数都是相同的，那么最大公约数也会相同。
>
> 所以得到式子 $\gcd(a,b)=\gcd(b, a \bmod b)$

```
int gcd(int a, int b) { return b == 0 ? a : gcd(b, a % b); }
```

性质

欧几里得算法的时间效率如何呢？下面我们证明，欧几里得算法的时间复杂度为 $O(\log n)$。

证明

当我们求 $\gcd(a,b)$ 的时候，会遇到两种情况:

- $a<b$，这时候 $\gcd(a,b)=\gcd(b,a)$;
- $a \geq b$，这时候 $\gcd(a,b)=\gcd(b, a \bmod b)$，而对 a 取模会让 a 至少折半。这意味着这一过程最多发生 $O(\log n)$ 次。

第一种情况发生后一定会发生第二种情况，因此第一种情况的发生次数一定 **不多于** 第二种情况的发生次数。

从而我们最多递归 $O(\log n)$ 次就可以得出结果。

最小公倍数

最小公倍数

接下来我们介绍如何求解最小公倍数（Least Common Multiple, LCM）。

定义

一组整数的公倍数，是指同时是这组数中每一个数的倍数的数。0 是任意一组整数的公倍数。

一组整数的最小公倍数，是指所有正的公倍数里面，最小的一个数。

两个数

设 $a = p_1^{k_{a_1}} p_2^{k_{a_2}} \cdots p_s^{k_{a_s}}$，$b = p_1^{k_{b_1}} p_2^{k_{b_2}} \cdots p_s^{k_{b_s}}$

我们发现，对于 a 和 b 的情况，二者的最大公约数等于

$p_1^{\min(k_{a_1},k_{b_1})} p_2^{\min(k_{a_2},k_{b_2})} \cdots p_s^{\min(k_{a_s},k_{b_s})}$

最小公倍数等于

$p_1^{\max(k_{a_1},k_{b_1})} p_2^{\max(k_{a_2},k_{b_2})} \cdots p_s^{\max(k_{a_s},k_{b_s})}$

由于 $k_a + k_b = \max(k_a, k_b) + \min(k_a, k_b)$

所以得到结论是 $\gcd(a, b) \times \operatorname{lcm}(a, b) = a \times b$

要求两个数的最小公倍数，先求出最大公约数即可。